UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/482,843	01/13/2000	Marcus Peinado	MSFT-0103/127334.6	7584

7590 05/11/2004

Steven H Meyer
Woodcock Washburn Kurtz Mackiewicz & Norris LLP
One Liberty Place
46th Floor
Philadelphia, PA 19103

EXAMINER	
NGUYEN, CUONG H	

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 05/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/482,843	PEINADO ET AL.
	Examiner	Art Unit
	CUONG H. NGUYEN	3625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *121,124 and 126-135* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *121,124 and 126-135* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is the answer to the RCE received on 2/11/2004.

2. Claims 121, 124, 126-135 are pending in this application.

Response

3. This Office Action is made NON-FINAL due to the arguments presented in the amendment (fax received on 2/27/2004), and new ground of rejections are presented herein.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C.§ 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

4. Re. To claim **121**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878).

Caronni et al. teach about a computer structure having various data fields (e.g., a first data field, a second data field, a third data field .etc., with encryption keys, and encrypted contents -see Caronni et al., the abstract, Fig.6, 9:10-21).

However, what contain in specific fields, i.e., "a first data field", "a second data field", "a third data field", "a fourth data field" of said computer-readable medium/floppy disk are considered as "non-functional descriptive material", they do not contribute further for a claimed structure for a medium/floppy disk, in

other words, they only explain more about an intent of use of those limitations, and they do not contribute to a further limitation of a claimed computer-readable medium.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement Caronni et al.'s ideas in a software program with further specific information, because claim 121 is merely directed to a computer-readable medium having multiple data fields; artisan in crypto field would appreciate to organize information to different fields containing extra information for a particular application.

5. Re. To claim **124**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of **Onoe** et al., US Pat. 5,951,642),or in view of Clark (US Pat. 6,343,280), or in view of Coley et al. (US Pat. 5,790,664).

The rationales and references for rejection of claim 121 are incorporated.

Onoe also teaches that a provider location is a network address/Internet address (see **Onoe** et al.); (or see Clark, in Detailed Description Text portion (para. 38):

"FIG. 14 depicts a block diagrammatic overview of the operation of the Trap Software 6 determining, connecting to, and executing the Modified Software 7 in cooperation with the License Server 4 (selected from a set of available License Server's 4) having the fastest network response time at the time of the Trap Software's 6 request for service from the License Server 4. In order to locate the fastest network route to a License Server 4, software object 266 (contained within the Trap Software 10) communicates 264 a "ping" message to each License Server 4 known to software object 266 in order to determine which License Server 4 has the fastest network response time. A "ping" measures the amount of time it takes a

small packet of bytes to travel to and from a given network address, in this instance the address of each of the known License Servers 4. By measuring the average ping time to each License Server 4, an estimate can be formed as to which License Server 4 will provide the fastest service for the Trap Software's 6 request. Software object 266 communicates 274 the ping information (network address of the License Server 4 providing the quickest response time) to software object 267 which then acts to make a network connection from the Software User 2 to the best (smallest average ping time) License Server 4. Software object 267 communicates 268 to software object 25 that the connection to the License Server 4 has been established, and software object 25 begins executing the Modified Software 7. The Modified Software 7 continues to execute as described previously until a Trap/Breakpoint is encountered or the execution terminates. While the Modified Software 7 executes, software object 25 periodically communicates 276 to software object 269 the request to search for the License Server 4 having the quickest network response time. Software object 269 communicates 265 an identical ping query to each of the known License Servers 4. The results of the network ping query is communicated 277 by software object 269 to software object 270 which checks to see if a faster route to a License Server 4 was found. If software object 270 determines that a faster route than the route to the currently connected License Server 4 was found, then the network address of the License Server 4 having the faster ping query response time is communicated 278 by software object 270 to software object 271 which terminates the connection with the License Server 4 having the slower ping query response time and makes a connection to the License Server 4 having the faster ping query response time. Software object 271 then communicates 272 a control signal to software object 269 where the process of making a ping query of all known License Servers 4 is repeated periodically while the Modified Software 7 continues to execute. If software object 270 determines that a faster route (a network connection having a lower ping query response time) to a License Server 4 was not found, then software object 270 does not communicate 278 a new License Server 4 network address to software object 271 whereby the Software User 2 stays connected to the previously selected License Server 4 and software object 270 communicates 273 a reset signal to software object 269. In this manner, the Trap Software 6 always maintains a connection" .

Or Coley et al. also teach that a license provider location is a network address. (e.g., see Coley et al. - in Detailed Description Text portion (para.8): "Once the connection is confirmed (step 206), the client module 103 forms a license validity inquiry request message (step 208). The request message may contain information such as the application name, the application version number, a date/time stamp, the name of a license server 110 (if several license servers are maintained by the software provider), and a hardware identifier, such as the IP address of the computer 100 ».

It would have been obvious to one of ordinary skill in the art at the time of invention to combine Caronni et al., **Onoe** et al., or Clark, or Coley et al.'s ideas with further specific information that is necessary for a transaction such as information about a provider Internet address.

6. Re. To claim **126**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Downs et al., (US Pat.6,574,609).

The rationales and references for rejection of claim 121 are incorporated.

Downs et al. further teach that a public key is encrypted (see Downs et al., Brief Summary Text (14):

It is an object of the present invention to remove the above-mentioned drawbacks and to provide a secure electronic content management system. One embodiment of the present invention provides a method of managing content data and associated metadata. According to the method, the content data and the associated metadata are generated. The content data is transferred to a content host, and the metadata and usage condition data for the associated content are transferred to an electronic store. The metadata and/or the usage condition data are altered in order to form promotional data, and the promotional data is transferred from the electronic store to a customer's system. In one preferred method, the content data is

encrypted with a first encrypting key before being transferred to the content host. The first encrypting key is encrypted with a second encrypting key, and the encrypted first encrypting key is transferred along with the metadata and usage condition data to the electronic store. Additionally, the encrypted first encrypting key is transferred along with the promotional data to the customer's system.) ; Or Epstein teaches that a provider's public key is encrypted (see Epstein, the summary and claim 1).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Caronni et al., and Downs et al. 's ideas in a computer-readable medium, because artisan in this specific field would appreciate that electronic communication is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

7. Re. To claim **127**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Downs et al., (US Pat.6,574,609), and further in view of Ganesan (US Pat. 5,535,276), or **Sudia** (US Pat. 6,009,177).

The rationales and references for rejection of claim 126 are incorporated.

Ganesan further teaches that a encrypted public key is signed by a private key, ["and wherein alteration of the encrypted content provider public key prevents validation of the data structure" – please note that this phrase (in double quotes) is merely an intent of use of claimed "encrypted public key", it does not contribute to a structural limitation of a claimed computer-readable medium]. Sudia also teaches that an **encrypted** public key is signed by a private key (note: "and wherein alteration of the encrypted content provider public key prevents validation of the package" is a "functional description phrase", it would not be considered having weight for such a computer-readable medium claim) (e.g. see **Sudia** US Pat. 6,009,177 "Brief Summary Text (13):

Another system of digital signature, called DSA for Digital Signature Algorithm, may also be used for sender verification. The DSA Algorithm was disclosed in U.S. patent application Ser. No. 07/738,431, which is hereby incorporated by reference in its entirety. The DSA Algorithm has properties that are similar to those of the RSA signature algorithm in that the sender passes the message through a hashing algorithm to produce a message digest and then encrypts or signs the message digest using his private key; the recipient verifies the encrypted digest using the-sender's public key. However, unlike the RSA signature algorithm that returns the original message digest when the recipient decrypts the signature block, the DSA verification algorithm results only in a positive confirmation of the validity of the signature; communications encrypted using an intended recipient's public key cannot later be recovered by decryption with the recipient's corresponding private key. For this reason, the DSA algorithm may be used quite capably for digital signatures, but not for key transport or for direct message encryption".

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Caronni et al., Downs et al., and Ganesan or Sudia's ideas in a computer-readable medium, because artisan in this specific

field would appreciate that electronic communication is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

8. Re. To claim **128**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Ganesan (US Pat. 5,535,276).

The rationales and references for rejection of claim 121 are incorporated.

Ganesan further teaches that a public key is signed by the content provider private key, ["wherein alteration of the content provider public key prevents validation of the data structure" – please note that this phrase (in double quotes) is merely an intent of use of claimed "public key", it does not contribute to a structural limitation of a computer-readable medium] .

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Caronni et al., and Ganesan's ideas in a computer-readable medium, because artisan in this specific field would appreciate that electronic communication is assumed to be unsecured, all

communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

9. Re. To claims 133, 134: They are rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Geer Jr. et al., (US Pat. 6,212,634), or in view of Sudia et al., US Pat. 5,995,625).

The rationales and references for rejection of claim 121 are incorporated.

10. Re. To claim 134: The rationales and references for rejection of claim 121 are incorporated.

- a first certificate and a second certificate having their public keys (note: this claim would be interpreted like the above because it is directed to a physical medium and what possess by a content provider (or an intermediary source) is not part of the claimed package) (e.g., see Geer Jr. et al., "Detailed Description Text (para. # 31):

In the event that there are multiple conversations between multiple subsets of the computers monitored by the arbiter, the arbiter can create a set of conversation certificates corresponding to each of the respective conversations. For example, if initially there is a conversation between two of the computers and then

three additional computers join in, the arbiter can initially create a conversation certificate for the two computers, which it distributes to the two computers only, and then when the arbiter is notified that three additional computers will be joining, the arbiter creates a new conversation certificate and distributes it to all five computers. The arbiter records, as the final entry in the message log for the first conversation, a link to the message log for the second conversation, encrypted with the private key for the first conversation, which the arbiter then destroys. The arbiter records, as the first entry in the message log for the second conversation, a link to the message log for the first conversation, encrypted with the private key for the second conversation. The two parties to the first conversation can read the first message log by decrypting the messages using the public key contained in the first certificate, and all five parties can read the second message log by decrypting the messages using the public key contained in the second certificate.").

- Or Sudia et al. teach about a package with a first certificate and a second certificate (note: claim would be interpreted like the above because this claim is directed to a physical medium; it would be old and well-known that a certificate represents an authorization), (e.g., see Sudia et al., claim 41).

Or Sudia et al. teach that a provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider – please note that the following claimed information "... wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key," do not contribute to a content of claimed physical medium; therefore, they are not contribute to a limitation of that claim.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Caronni et al., and Geer Jr. et al., or with Sudia's ideas in a computer-readable medium, because artisan in this specific field would appreciate that electronic communication is assumed to be unsecured, therefore, a computer-readable medium having certificates would be used for security.

11. Re. To claim 133: It claims a medium having data fields with 2 certificates; the other information in this claim merely explain where and how these certificate are about, they do not contribute to said structural components (a computer-readable medium); therefore, claim 135's limitations cover limitations of claims 133-134 (i.e., a computer-readable medium contains multiple data field, such as a fourth data field containing a 1st certificate, a fifth data field containing a 2nd certificate, see above cited portion of Geer Jr. et al.).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Caronni et al., Geer Jr. et al., and Sudia's ideas in a computer-readable medium, because artisan in this specific field would appreciate that electronic communication is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public

keys are those that are distributed to others. Private keys are maintained in confidence.

12. Re. To claims 135, 129, 130 -132:

A. Re. To claim **135**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), Geer Jr. et al., (US Pat. 6,212,634), or in view of Sudia et al., US Pat. 5,995,625), in view of Simms III, (US Pat. 6,550,011), in view of Gruse et al. (US Pat. 6,389,538), and further in view of **Mullor** et al., (US Pat. 6,411,941),

The rationales and references for rejection of claim 134 are incorporated.

- a public key and a private key (see Caronni et al." *Brief Summary Text (13): An example of a key management system directed to unicast communications is the simple key management for Internet protocols (SunScreen.TM. SKIP, (SunScreen is a trademark of Sun Microsystems, Inc.). SKIP is a public key certificate-based key-management scheme which provides group key-management for Internet protocols. Prior multicast implementations of SKIP create a single multicast group. Designed to be application independent, SKIP can be plugged into the IP Security Protocol (IPSP) or IPV6. Using certified Diffie/Hellman keys, SKIP obviates the need for pseudo session state establishment and for prior communications between two participating ends in order to acquire and update traffic keys. One advantage of a public-key encryption that is particularly suited to connectionless datagram protocols such as the Internet protocol. In the SKIP system, each participant has the capability to construct a shared secret based only on knowledge of the other participants' public key combined with its own private key.*", or see Simms III, the abstract),

- a certificate is signed with a private key (see cited Gruse for a rejection of pending claim 132 about this limitation, below) ;
- a public key to decrypt the encrypted signature (this limitation is similar to a limitation of claim 127, or 132, 134; therefore, see cited Mullor for a rejection of this limitation in pending claim 129, or cited Sudia for a rejection of pending claim 127, or cited Geer for a rejection of pending claims 132, 134);

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the ideas of Caronni et al., Simms III, Gruse et al., and **Mullor** et al., Geer Jr. et al., or Sudia et al., because artisans in this specific field would appreciate these disclosed information are fundamental in a data structure in keeping security for a digital right management system.

B. Re. To claim **129**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Simms III, (US Pat. 6,550,011), or in view of **Mullor** et al., (US Pat. 6,411,941).

The rationales and references for rejection of claim 121 are incorporated.

- The data structure of claim 121 further comprising a field containing a key ID identifying the decryption key.

- This claim's limitation is merely about a computer-readable medium having an explanation of key, i.e., a public-key that is used for decryption (e.g., a license information in that medium is encrypted and obviously having a public-key to decrypt (see **Mullor** et al., claim 15).

Sims III also teaches about an ID for a decryption key (e.g., see Sims III, "Detailed Description Text (28):

The most preferred embodiment compliant information storage device also includes secure areas for storing one or more secure data sets. Such data sets may include an identification of the data set, such as a simple enumeration, content decryption keys, content use information, and public keys and their corresponding signatures. These data sets are preferably associated with particular protected works, providing association to the content of content keys and information regarding any restrictions on use of the content (content use information).").

C. Re. To claim **130**: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Simms III, (US Pat. 6,550,011).

The rationales and reference for rejection of claim 121 are incorporated.

- a fourth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the data structure (claim 135 obviously is directed toward a data field having a certificate – please note that "a certificate from the root source indicating that the content provider has authority from the root source to provide the data structure" is merely an intend of use for claimed "certificate" ", it does not contribute to a structural limitation of a claimed computer-readable medium.

- Sims III also teaches a certificate (in said package) corresponding to a provider (see Sims III, "Detailed Description Text (48):

"Transmission of the certificates is particularly useful in situations where the destination device is a less known device, such as provided by a relatively small company or is a relatively new device, and does not appear on the source device's list of acceptable devices. If the certificate is provided by a certificate authority that the content provider trusts, the certificate should be acceptable proof of the device's compliance.").

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the ideas of Caronni et al., Simms III because artisans in

this specific field would appreciate these disclosed information are fundamental in a data structure in keeping security for a digital right management system.

D. Re. To claim 131: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Simms III, (US Pat. 6,550,011), and further in view of Wiser et al., (US Pat. 6,385,596).

The data structure of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider. Claim 135 obviously contains a limitation of a certificate comprises a public key. Therefore, it is rejected on the same rationales and references as in claim 135.

- Wiser et al. also teach that a certificate having a public key provider (see Wiser et al., "Detailed Description Text (29):

Referring to FIG. 4 there is shown an embodiment of a passport. Each passport includes a consumer certificate 402, a consumer private key 412, encrypted personal information 414, and a registration key 420. The consumer certificate 402 is used to authenticate the purchaser of a media data file 200, and to encrypt a purchased media data file 200. The certificate 402 is preferably in the ISO X.509 format, and issued by a trusted certificate authority, which in the preferred embodiment is the media licensing center 110. Each consumer certificate 402 in the ISO X.509 format includes a consumer public key 404, set of validity dates 406 defining the period during which the certificate is valid, a serial number 408, and a digital signature 410 of certificate authority."; or see Sims III, "Detailed Description Text (63):

At step 307 the computer provides to the storage device the public key for the acceptable use device and/or a certificate from an acceptable certificate authority. The storage device will preferably verify the public key and/or certificate and encrypt future communication with that public key or the public key associated with the certificate.").

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the ideas of Caronni et al., Simms III, and Wiser because artisans in this specific field would appreciate these disclosed useful information are fundamental in a data structure in keeping security for a digital right management system.

E. Re. To claim 132: It is rejected under 35 U.S.C.§ 103(a) as being unpatentable over Caronni et al. (US Pat. 6,049,878), in view of Simms III, (US Pat. 6,550,011), in view of Wiser et al., (US Pat. 6,385,596), and further in view of Gruse et al. (US Pat. 6,389,538).

The rationales and references for rejection of claim 131 are incorporated.

- Gruse et al. teach that a certificate is signed with a private key (note: "and wherein alteration of the encrypted content provider public key prevents validation of the package" is not contributing a structural component 's limitation of this claim (e.g., see Gruse et al., "Detailed Description Text (359):

Electronic Digital Content Store(s) Certificate--A certificate provided to the Electronic Digital Content Store(s) 103 by the Clearinghouse(s) 105 and signed by the Clearinghouse(s) 105 using its private key. This certificate is used by the End-User Player Application 195 to verify that the Electronic Digital Content Store(s) 103 is a valid distributor of Content 113. The End-User Player Application 195 and Clearinghouse(s) 105 can verify that the Electronic Digital Content Store(s) 103 is an authorized distributor by decrypting the certificate's signature with the Clearinghouse's 105 Public Key 621. The End-User Player Application 195 keeps a local copy of the Clearinghouse's 105 Public Key 621 that it receives as part of its initialization during installation.").

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the ideas of Caronni et al., Simms III, Wiser et al., and Gruse et al. because artisans in this specific field would appreciate these disclosed useful information are fundamental in a data structure in keeping security for a digital right management system.

Conclusion

13. Claims 121, 124, 126-135 are not patentable.

14. Note: Since the examiner is examining an utility patent, the claims must be directed to systems, methods or articles of manufacture that have a clear utility. See MPEP 706.03(a) for example. Over the years, numerous court decisions have analyzed the content of various claimed language for meaningful, useful differences in structure or acts performed between the claims and the prior art. Some of these decision have found that certain language adds little, if anything, to the claimed structure or acts and thus do not serve as a limitation on the claims to distinguish over the prior art. For example, language directed to an intended use for a system of in a claim that does not result much in a structural or functional difference with respect to prior art were held not to serve as a limitation on the claim. See in re **Schreiber**, 44 USPQ2d 1429 (CAFC 1997).

Thus, a limitation on a claim can broadly be thought of then as its ability to make a meaningful contribution to the definition of the invention in a claim. In other words, language that is not functionally interrelated with the useful acts, structure, or properties of the claimed invention will not serve as a limitation. See in re **Gulack**, 217 USPQ 401 (CAFC 1983), ex parte **Carver**, 227 USPQ 465 (BdPatApp&Int 1985) and in re **Lowry**, 32 USPQ2d 1031 (CAFC 1994) where language provided certain limitations because of specific relationships required by the claims.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CUONG H. NGUYEN whose number is 703-305-4553. The examiner can normally be reached on 7am-3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's acting supervisor, JEFFREY A. SMITH can be reached on 703-308-3588. The fax phone number for the organization where this application or proceeding is assigned is 703-305-7687.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Cuonghnguyen

CUONG H. NGUYEN
Primary Examiner
Art Unit 3625